Nom : _____ Date : _____ Note : _____

Bases de la cybersécurité et prévention des menaces Prévention

Menaces de cybersécurité, pare-feu réseau, authentification multifacteur, cadres de sécurité

PRÉSENTATION DES BASES DE LA CYBERSÉCURITÉ

SÉCURISÉ

CHIFFREMENT DES DONNÉES

Norme AES 256 bits

CONFORME

NORMES MONDIALES

Cadres RGPD (GDPR) et CCPA

ZERO TRUST

POLITIQUE D'ACCÈS

Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers les principes fondamentaux de la cybersécurité et de la prévention des menaces en ligne. Vous étudierez les menaces liées aux logiciels malveillants, l'authentification multifacteur, les pare-feu réseau et les cadres de réponse aux incidents.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/

Votre parcours d'apprentissage : bases de la cybersécurité

- Identifier les vecteurs courants de logiciels malveillants, d'hameçonnage et d'intrusion dans les réseaux d'entreprise.
- Mettre en œuvre les contrôles de cybersécurité standard, notamment la MFA, les pare-feu et la protection des terminaux.
- Évaluer les procédures de réponse aux incidents pour atténuer l'impact des violations de données.
- Analysez les facteurs de risque organisationnels et l'alignement de la sécurité sur les lignes directrices du NIST.
- Mettez en place de bonnes pratiques d'hygiène de sécurité pour limiter le credential stuffing automatisé.

INSTRUCTIONS DU GUIDE DE CYBERSÉCURITÉ

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la prévention des menaces. Terminez par l'activité bonus Réflexion rapide.

BASES DE LA CYBERSÉCURITÉ ET PRÉVENTION DES MENACES (INTRODUCTION)

La cybersécurité protège les réseaux, les systèmes et les données contre les attaques numériques non autorisées. Adopter de solides habitudes de sécurité, configurer des pare-feu, exiger l'authentification multifacteur et former le personnel à reconnaître les menaces sont des éléments essentiels de la défense du réseau d'une entreprise.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1 **1. Quel est l'objectif principal d'une attaque d'hameçonnage ?**

- A. Voler des identifiants et des données sensibles des utilisateurs
- B. Améliorer la visibilité du site web dans les moteurs de recherche
- C. Augmenter la capacité de bande passante du réseau
- D. Gérer la réplication des centres de données de sauvegarde

2 **2. Quel mécanisme offre la protection de compte la plus solide ?**

- A. Authentification multifacteur à l'aide de clés matérielles
- B. Des mots de passe complexes changés tous les trente jours
- C. Limiter la connexion au compte aux heures de bureau
- D. Masquer le nom d'utilisateur du compte dans les annuaires publics

3 **3. Qu'est-ce qui définit la charge utile d'une infection par rançongiciel ?**

- A. Chiffrer les fichiers système et exiger un paiement
- B. Enregistrer discrètement les frappes au clavier et les envoyer à des serveurs distants
- C. Injecter de la publicité non autorisée dans les navigateurs
- D. Utiliser les ressources du processeur local pour miner de la cryptomonnaie

4 **4. Quel est l'impact d'un exploit zero-day sur les défenses de sécurité ?**

- A. Il cible des vulnérabilités inconnues et non corrigées
- B. Il désactive automatiquement le pare-feu de l'entreprise
- C. Il force le système à effectuer un redémarrage complet
- D. Il ne nécessite aucun budget pour y remédier

5 **5. Quel cadre régit les contrôles de sécurité en entreprise ?**

- A. Lignes directrices du NIST Cybersecurity Framework
- B. Spécifications W3C du schéma de document HTML5
- C. Manuels d'installation de pilotes d'imprimante
- D. Définitions de protocoles de routage de l'IETF

Point de contrôle 2 : Défi Vrai ou Faux

6 Question vrai/faux 6

6. Les attaques par hameçonnage ne visent que les comptes de messagerie personnels.

- ◯ Vrai
- ◯ Faux

7 Question vrai/faux 7

7. L'authentification multifacteur aide à bloquer les attaques par bourrage d'identifiants (credential stuffing).

- ◯ Vrai
- ◯ Faux

8 Question vrai/faux 8

8. Les pare-feu inspectent le trafic réseau pour bloquer les accès non autorisés aux ports.

- ◯ Vrai
- ◯ Faux

9 Question vrai/faux 9

9. La correction des exploits zero-day nécessite des mises à jour standard des définitions antivirus.

- ◯ Vrai
- ◯ Faux

10 Question vrai/faux 10

10. Un honeypot est un serveur leurre utilisé pour attirer les cybercriminels.

- ◯ Vrai
- ◯ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Les administrateurs réseau installent un _____ pour filtrer le trafic entrant.

2. Un attaquant utilise un _____ zero-day pour contourner les correctifs du système.

3. Les attaquants envoient des e-mails usurpés pour mener contre les employés des campagnes d' _____ .

4. Le rançongiciel est une forme destructrice de _____ qui verrouille les données des utilisateurs.

5. Instaurer une bonne _____ des mots de passe réduit les risques de vol d'identifiants.

6. Pour protéger les communications sensibles, les utilisateurs appliquent des protocoles de _____ .

BANQUE DE MOTS DE VOCABULAIRE

CHIFFREMENT EXPLOIT HAMEÇONNAGE HYGIÈNE LOGICIEL MALVEILLANT MULTIFACTEUR PARE-FEU RANÇONGICIEL

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.

Point de contrôle 4 : Association de notions sur la sécurité

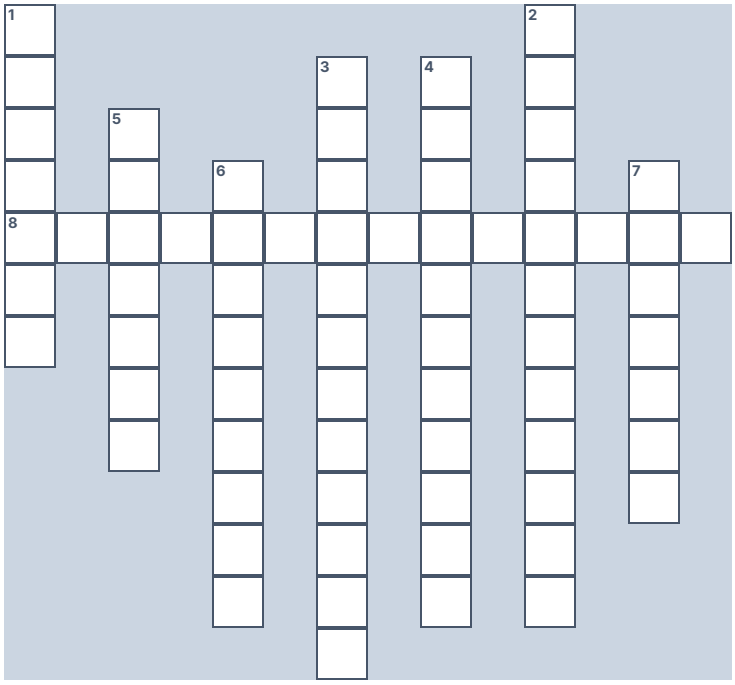
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. Menace de rançongiciel	**A**	Lignes directrices structurées, comme celles du NIST, utilisées pour gérer les cyberrisques.
☐	2. Authentification multifacteur	**B**	Plan structuré pour gérer et atténuer les failles de sécurité.
☐	3. Exploit zero-day	**C**	Barrière réseau qui filtre le trafic selon des règles de sécurité.
☐	4. Leurre (honeypot)	**D**	Logiciel malveillant qui chiffre les données et exige un paiement pour les déchiffrer.
☐	5. Pare-feu anti-intrusion	**E**	Exploitation d'une vulnérabilité ciblée avant la publication d'un correctif par l'éditeur.
☐	6. Réponse aux incidents	**F**	Bonnes pratiques de gestion des identifiants et des clés d'authentification.
☐	7. Hygiène des mots de passe	**G**	Validation de sécurité exigeant au moins deux facteurs d'authentification.
☐	8. Cadre de sécurité	**H**	Système leurre mis en place pour attirer et analyser des acteurs malveillants.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

8. Exploitation d'une vulnérabilité ciblée avant la publication d'un correctif par l'éditeur (14)

VERTICALEMENT

1. Bonnes pratiques de gestion des identifiants et des clés d'authentification (7)

2. Logiciel malveillant qui chiffre les données et exige un paiement pour les déchiffrer (12)

3. Validation de sécurité exigeant au moins deux facteurs d'authentification (12)

4. Lignes directrices structurées, comme celles du NIST, servant à gérer les cyberrisques (11)

5. Plan structuré de gestion et d'atténuation des failles de sécurité (7)

6. Système leurre mis en place pour attirer et analyser les acteurs malveillants (9)

7. Barrière réseau qui filtre le trafic selon des règles de sécurité (7)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

8 horizontal: Exploitation d'une vulnérabilité ciblée avant la publication d'un correctif par l'éditeur (14 lettres):

VERTICALEMENT

1 vertical: Bonnes pratiques de gestion des identifiants et des clés d'authentification (7 lettres):

2 vertical: Logiciel malveillant qui chiffre les données et exige un paiement pour les déchiffrer (12 lettres):

3 vertical: Validation de sécurité exigeant au moins deux facteurs d'authentification (12 lettres):

4 vertical: Lignes directrices structurées, comme celles du NIST, servant à gérer les cyberrisques (11 lettres):

5 vertical: Plan structuré de gestion et d'atténuation des failles de sécurité (7 lettres):

6 vertical: Système leurre mis en place pour attirer et analyser les acteurs malveillants (9 lettres):

7 vertical: Barrière réseau qui filtre le trafic selon des règles de sécurité (7 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

L K T S V R Z E H E S C A L Q
E L E I T N E R E F E R C R P
I Z M K H Y G I E N E V E A R
C U A S W J M M H H N P R H R
I F K T L R W H B U O E F Y O
G Y W S H T X A P N F U N N Z
N O I Q T I P V S E U O U U K
O A E P M K A E U N V G G P Q
C X Y J K V J Y W Y P J I Z I
N J N L E I M E D T O P A E I
A E X P L O I T Z E R O D A Y
R A S A J F W E K Z K E K Q N
J A M U L T I F A C T E U R F
O K N D N C D H I B A P R L P
W T I Y F Y S G X W H F R T N

LISTE DE MOTS DE VOCABULAIRE

RANCONGICIEL MULTIFACTEUR EXPLOITZERODAY POTDEMIEL PAREFEU
REPONSE HYGIENE REFERENTIEL

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. RANCONGICIEL
B. MULTIFACTEUR
C. EXPLOITZERODAY
D. POTDEMIEL
E. PAREFEU
F. REPONSE
G. HYGIENE
H. REFERENTIEL

DÉFINITIONS ET CHAMPS D'ASSOCIATION
____ 1. Barrière réseau qui filtre le trafic selon des règles de sécurité.
____ 2. Plan structuré de gestion et d'atténuation des failles de sécurité.
____ 3. Logiciel malveillant qui chiffre les données et exige un paiement pour les déchiffrer.
____ 4. Validation de sécurité exigeant au moins deux facteurs d'authentification.
____ 5. Bonnes pratiques de gestion des identifiants et des clés d'authentification.
____ 6. Lignes directrices structurées, comme celles du NIST, servant à gérer les cyberrisques.
____ 7. Exploitation d'une vulnérabilité ciblée avant la publication d'un correctif par l'éditeur.
____ 8. Système leurre mis en place pour attirer et analyser les acteurs malveillants.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. CNIOAGIRENLC
2. OXIPTAEDZYROEL
3. EPFUREA
4. EYEINHG
5. UECARLITFMUT
6. EDOIMPELT
7. RSNEEOP
8. INLEFRREETE

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Métiers de la cybersécurité			
2	Raisons de mettre à jour les logiciels			
3	Choses qu'un pare-feu peut bloquer			
4	Signaux d'alerte dans un e-mail			
5	Choses que vous sauvegardez			
6	Types de cyberattaques connus			
7	Choses qu'un honeypot peut attirer			
8	Informations que vous ne devriez jamais partager			
9	Signes qu'un ordinateur est infecté			
10	Films ou séries sur les hackers			
11	Couches de sécurité que vous pouvez mettre en place			
12	Choses à pratiquer lors d'un exercice de sécurité			
13	Outils de sécurité que vous connaissez			
14	Personnes à qui demander de l'aide informatique			
15	Mots qui commencent par 'cyber'			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : STRATÉGIE DE RESTAURATION APRÈS UN RANÇONGICIEL



Scénario : Un réseau d'entreprise est infecté par un rançongiciel qui verrouille des bases de données critiques. Les attaquants exigent un paiement de $100,000 en cryptomonnaie. L'entreprise dispose de sauvegardes hors ligne datant de 24 heures.

Question de discussion : analysez les risques liés au paiement et évaluez la stratégie de récupération.

ÉTUDE DE CAS 2 : DÉFENSES CONTRE LE CREDENTIAL STUFFING



Scénario : Un service en ligne subit une attaque par bourrage d'identifiants, au cours de laquelle des pirates testent des millions de paires nom d'utilisateur/mot de passe volées sur d'autres sites.

Question de discussion : Détaillez le mécanisme de cette attaque et décrivez deux systèmes de défense.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

19	5	3	21	18	9	19	5	26		20	15	21	20		16	1	18
1	21	20	8	5	14	20	9	6	9	3	1	20	9	15	14		
13	21	12	20	9	6	1	3	20	5	21	18						

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Quel est l'objectif principal de la cybersécurité ?

L'objectif principal est de protéger les réseaux, les appareils et les données contre les accès non autorisés, les attaques et les dommages accidentels.

Q2: En quoi l'hameçonnage diffère-t-il du spear phishing ?

L'hameçonnage est une campagne d'e-mails à grande échelle visant des utilisateurs au hasard, tandis que le spear phishing vise des personnes précises à l'aide de données personnalisées.

Q3: Qu'est-ce qu'un pare-feu réseau ?

Un pare-feu est un système de sécurité réseau qui surveille et filtre le trafic entrant et sortant selon des règles de sécurité prédéfinies.

Q4: Pourquoi l'authentification multifacteur (MFA) est-elle nécessaire ?

La MFA ajoute une couche de défense essentielle, qui empêche l'accès même si des attaquants volent ou cassent le mot de passe principal.

Q5: Qu'est-ce qui définit un virus informatique ?

Un virus est un logiciel malveillant auto-réplicatif qui s'attache à des fichiers sains et se propage d'un système à l'autre une fois exécuté.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Comment un rançongiciel verrouille-t-il les données locales ?

Les rançongiciels utilisent des algorithmes cryptographiques pour chiffrer les fichiers des utilisateurs, les rendant illisibles jusqu'à l'application d'une clé de déchiffrement.

Q7: Qu'est-ce qu'une vulnérabilité zero-day ?

Une faille zero-day est une faille de sécurité d'un logiciel inconnue de l'éditeur, qui ne laisse aucun délai pour développer un correctif avant son exploitation.

Q8: Quel est le rôle du cadre du NIST ?

Le cadre du NIST fournit des lignes directrices et des normes volontaires pour aider les organisations à gérer et à réduire les risques de cybersécurité.

Q9: Qu'est-ce qu'un plan de réponse aux incidents de sécurité ?

Il s'agit d'un ensemble documenté de procédures pour détecter et contenir les failles de sécurité et les compromissions du réseau, puis s'en remettre.

Q10: Comment l'ingénierie sociale exploite-t-elle les utilisateurs ?

L'ingénierie sociale utilise la manipulation psychologique pour amener des employés à révéler leurs mots de passe ou à télécharger des fichiers malveillants.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment une attaque DDoS submerge-t-elle les serveurs Web ?

Une attaque DDoS coordonne des millions d'appareils compromis d'un botnet pour inonder un serveur de trafic et épuiser sa bande passante et ses capacités processeur.

Q2: Quelle est la différence entre chiffrement symétrique et asymétrique ?

Le chiffrement symétrique utilise une seule clé pour chiffrer et déchiffrer, tandis que le chiffrement asymétrique utilise une paire de clés publique et privée.

Q3: Comment les pirates mènent-ils des attaques par injection SQL ?

Les attaquants saisissent des commandes SQL malveillantes dans des champs de formulaire, amenant la base de données du serveur à divulguer des enregistrements d'utilisateurs sans autorisation.

Q4: Qu'est-ce que le mouvement latéral dans les intrusions réseau ?

Il s'agit de la technique par laquelle les attaquants exploitent un accès initial à un serveur pour compromettre d'autres systèmes interconnectés du réseau interne.

Q5: Comment l'usurpation DNS (DNS spoofing) redirige-t-elle le trafic web ?

L'usurpation DNS modifie les enregistrements du cache des serveurs de noms et redirige les utilisateurs légitimes vers des sites malveillants imitant les domaines visés.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Qu'est-ce qu'un jeton de sécurité matériel ?

Il s'agit d'un appareil physique (comme une YubiKey) qui génère des preuves d'authentification cryptographiques, offrant une défense maximale contre l'hameçonnage à distance.

Q7: Comment les équipes de sécurité utilisent-elles des pots de miel (honeypots) leurres ?

Les équipes déploient des serveurs leurres hors production pour détecter les intrusions tôt et analyser les schémas d'attaque des acteurs non autorisés.

Q8: Qu'est-ce que le principe du moindre privilège ?

Il s'agit de la règle de sécurité consistant à limiter les droits d'accès des utilisateurs au strict minimum nécessaire à leurs fonctions.

Q9: Comment une attaque de l'homme du milieu exploite-t-elle les connexions ?

Un attaquant intercepte et modifie les communications entre deux appareils sur des réseaux non chiffrés, et vole des jetons de session et des identifiants.

Q10: Que sont les indicateurs de compromission (IOC) ?

Les IOC sont des indices forensiques, comme des modifications inhabituelles du registre ou un trafic IP suspect, qui montrent qu'un système a été compromis.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

Les attaquants analysent en permanence Internet à la recherche de serveurs vulnérables et envoient des e-mails d'hameçonnage (phishing) dans les boîtes de réception des employés.

2. APERÇU SÉCURITÉ

L'erreur humaine, comme cliquer sur des liens d'hameçonnage, est un facteur fréquent des violations de données, d'où l'importance de la formation.

3. APERÇU SÉCURITÉ

Le coût d'une violation de données comprend les amendes, la perte de clients, l'enquête et la remise en état, et peut atteindre plusieurs millions de dollars.

4. APERÇU SÉCURITÉ

La MFA résistante à l'hameçonnage, comme les clés de sécurité matérielles, est le type de MFA le plus solide et la norme recommandée par la CISA. [2]

5. APERÇU SÉCURITÉ

Les rançongiciels restent une menace majeure pour les réseaux d'entreprise, et la CISA recommande vivement des sauvegardes hors ligne chiffrées comme défense essentielle. [4]

6. APERÇU SÉCURITÉ

Le NIST Cybersecurity Framework 2.0 (2024) comporte six fonctions essentielles : Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. ZOOM SUR LA SÉCURITÉ

Les robots de credential stuffing testent à grande échelle des paires de noms d'utilisateur et de mots de passe divulgués sur les portails de connexion des banques et des sites marchands.

8. ZOOM SUR LA SÉCURITÉ

Des marchés d'exploits zero-day existent dans le monde entier, où des vulnérabilités de haute gravité peuvent se vendre très cher avant d'être corrigées.

9. ZOOM SUR LA SÉCURITÉ

Un système leurre (honeypot) signale immédiatement les intrusions, puisque les utilisateurs légitimes n'ont aucune raison d'y accéder.

10. APERÇU SÉCURITÉ

Transport Layer Security (TLS) chiffre les sessions du navigateur, ce qui empêche l'interception de paquets (sniffing) sur les réseaux Wi-Fi publics.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Corrigé : Point de contrôle 1 – Choix multiple

1 **Attaques par hameçonnage** HAMEÇONNAGE — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les campagnes d'hameçonnage tentent de voler des identifiants et des données sensibles au moyen d'e-mails usurpés. Source : OWASP Secure Configuration.

2 **Protection du compte** CLÉ MFA — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

L'authentification multifacteur (MFA) avec jetons matériels offre la défense la plus solide pour l'accès aux comptes. Source : NIST Digital Identity.

3 **Menace des rançongiciels** RANÇONGICIEL — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les rançongiciels chiffrent les systèmes et données critiques et exigent un paiement en cryptomonnaie en échange des clés de déchiffrement. Source : Center for Internet Security (CIS).

4 **Vulnérabilité zero-day** ZERO-DAY — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les menaces zero-day exploitent des failles de sécurité inconnues et non corrigées avant qu'un correctif du fournisseur ne soit disponible. Source : OWASP Secure Configuration.

5 **Cadres de sécurité** CADRES — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Des cadres comme celui du NIST fournissent des lignes directrices structurées pour aider les organisations à gérer et réduire les cyberrisques. Source : NIST Digital Identity.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Hameçonnage ciblé** HAMEÇONNAGE — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les attaques par hameçonnage visent à la fois les réseaux d'entreprise et les comptes personnels pour multiplier les vecteurs d'exploitation. Source : OWASP Secure Configuration.

7 **Question 7** — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

La MFA exige un second facteur : un mot de passe volé ne suffit donc généralement pas à lui seul pour se connecter.

8 **Pare-feu de trafic** PARE-FEU — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les pare-feu inspectent et bloquent le trafic sur certains ports réseau afin de filtrer les connexions non autorisées. Source : Center for Internet Security (CIS).

9 **Réponse aux failles zero-day** ZERO-DAY — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Corriger les failles zero-day exige des correctifs de code et un filtrage par WAF, car les signatures n'existent pas encore. Source : OWASP Secure Configuration.

10 **Leurres (honeypots)** POT DE MIEL — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les pots de miel (honeypots) sont des serveurs leurres utilisés par les équipes de sécurité pour attirer, détecter et étudier les acteurs malveillants. Source : Center for Internet Security (CIS).

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

D 1. Menace de rançongiciel	G 2. Authentification multifacteur	E 3. Exploit zero-day	H 4. Leurre (honeypot)
C 5. Pare-feu anti-intrusion	B 6. Réponse aux incidents	F 7. Hygiène des mots de passe	A 8. Cadre de sécurité

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 PARE-FEU	2 EXPLOIT	3 HAMEÇONNAGE	4 LOGICIEL MALVEILLANT
5 HYGIÈNE	6 CHIFFREMENT		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 E – PAREFEU	2 F – REPONSE	3 A – RANCONGICIEL	4 B – MULTIFACTEUR
5 G – HYGIENE	6 H – REFERENTIEL	7 C – EXPLOITZERODAY	8 D – POTDEMIEL

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Menace de rançongiciel, Authentification multifacteur et Exploit zero-day avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

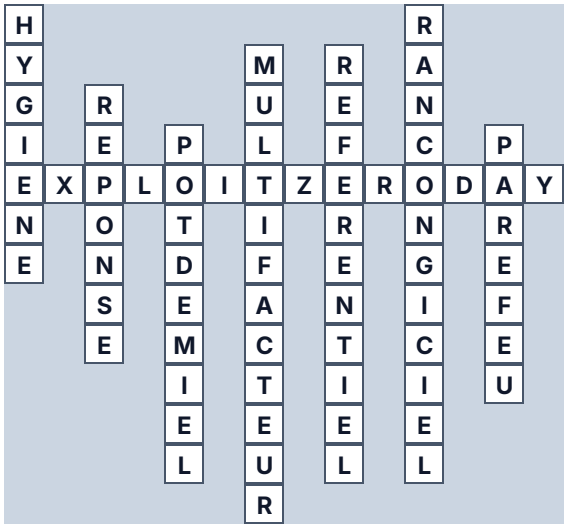
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

L	K	T	S	V	R	Z	E	H	E	S	C	A	L	Q
E	L	E	I	T	N	E	R	E	F	E	R	C	R	P
I	Z	M	K	H	Y	G	I	E	N	E	V	E	A	R
C	U	A	S	W	J	M	M	H	H	N	P	R	H	R
I	F	K	T	L	R	W	H	B	U	O	E	F	Y	O
G	Y	W	S	H	T	X	A	P	N	F	U	N	N	Z
N	O	I	Q	T	I	P	V	S	E	U	O	U	U	K
O	A	E	P	M	K	A	E	U	N	V	G	G	P	Q
C	X	Y	J	K	V	J	Y	W	Y	P	J	I	Z	I
N	J	N	L	E	I	M	E	D	T	O	P	A	E	I
A	E	X	P	L	O	I	T	Z	E	R	O	D	A	Y
R	A	S	A	J	F	W	E	K	Z	K	E	K	Q	N
J	A	M	U	L	T	I	F	A	C	T	E	U	R	F
O	K	N	D	N	C	D	H	I	B	A	P	R	L	P
W	T	I	Y	F	Y	S	G	X	W	H	F	R	T	N

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

8 horizontal: EXPLOITZERODAY Exploitation d'une vulnérabilité ciblée avant la publication d'un correctif par l'éditeur (14 lettres)

VERTICALEMENT

1 vertical: HYGIENE Bonnes pratiques de gestion des identifiants et des clés d'authentification (7 lettres)

2 vertical: RANCONGICIEL Logiciel malveillant qui chiffre les données et exige un paiement pour les déchiffrer (12 lettres)

3 vertical: MULTIFACTEUR Validation de sécurité exigeant au moins deux facteurs d'authentification (12 lettres)

4 vertical: REFERENTIEL Lignes directrices structurées, comme celles du NIST, servant à gérer les cyberrisques (11 lettres)

5 vertical: REPONSE Plan structuré de gestion et d'atténuation des failles de sécurité (7 lettres)

6 vertical: POTDEMIEL Système leurre mis en place pour attirer et analyser les acteurs malveillants (9 lettres)

7 vertical: PAREFEU Barrière réseau qui filtre le trafic selon des règles de sécurité (7 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. CNIOAGIRENLC — **RANCONGICIEL**
2. OXIPTAEDZYROEL — **EXPLOITZERODAY**
3. EPFUREA — **PAREFEU**
4. EYEINHG — **HYGIENE**
5. UECARLITFMUT — **MULTIFACTEUR**
6. EDOIMPELT — **POTDEMIEL**
7. RSNEEOP — **REPONSE**
8. INLEFRREETE — **REFERENTIEL**

CORRIGÉ DU DÉFI DU CODE SECRET

"SECURISEZ TOUT PAR AUTHENTIFICATION MULTIFACTEUR"

Corrigé des études de cas

A Étude de cas 1 : Stratégie de restauration après un rançongiciel

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : le réseau d'une entreprise est infecté par un rançongiciel qui verrouille des bases de données critiques. Les attaquants exigent un paiement de 100 000 $ en cryptomonnaie. L'entreprise dispose de sauvegardes hors ligne datant de 24 heures.
- Stratégie et solution recommandées : Risques du paiement : payer ne garantit pas le déchiffrement des fichiers, désigne l'entreprise comme une cible qui paie et finance des activités criminelles. Stratégie de reprise : l'équipe doit isoler les hôtes infectés, effacer les serveurs compromis et restaurer les données à partir de sauvegardes hors ligne. Elle doit corriger le vecteur d'accès initial (hameçonnage ou exploit) pour éviter une réinfection immédiate.

B Étude de cas 2 : Défenses contre le credential stuffing

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un service en ligne subit une attaque par bourrage d'identifiants (credential stuffing), au cours de laquelle des pirates testent des millions de paires nom d'utilisateur/mot de passe volées sur d'autres sites.
- Stratégie et solution recommandées : Mécanisme : les attaquants exploitent la réutilisation des mots de passe d'un site à l'autre en utilisant des robots automatisés pour se connecter aux comptes des utilisateurs. Défenses : 1. L'authentification multifacteur (MFA) bloque les tentatives de connexion même si le mot de passe est correct. 2. La mise en place d'une limitation du débit et de CAPTCHA bloque le trafic de robots automatisés qui inonde les points de connexion.